

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF:)

[REDACTED])
Cleveland, Ohio 44109)

Case No. 1:21 MJ 9129)

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Monica Hantz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed for over five years. I have received specialized training at the FBI Academy, in Quantico, Virginia, in a variety of Federal criminal violations, including training on how to conduct surveillance, conduct electronic and physical searches, interview and interrogation techniques, financial investigations (including asset forfeiture and money laundering tactics), evidence collection, weapons of mass destruction, arrest and search warrant executions, and case preparation. I am currently assigned to the FBI Cleveland Division Cyber Crimes Squad, which is responsible for investigations involving computer-related offenses. I am empowered to make arrests for federal offenses. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media

2. I am an “investigative or law enforcement officer” of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

EXHIBIT

B

3. I have probable cause to believe that evidence of a crime, fruits of a crime, contraband and instrumentalities of violations of: 18 U.S.C. § 2251 (Sexual Exploitation of Children); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (knowing possess, access, conspiracy to access, or attempted access with intent to view child pornography) are located within [REDACTED], Cleveland, Ohio (hereinafter the “SUBJECT PREMISES”). I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, as further described in Attachment A, and incorporated herein by reference, which is in the Northern District of Ohio. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to the knowing production, receipt, possession, distribution, access with intent to view, or reproduction of child pornography, as well as the attempt and conspiracy to violate the foregoing. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer, computer media, and mobile computing device located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

4. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/analysts and computer

forensic professionals; and my experience, training and background as a Special Agent (SA) with the FBI. This affidavit includes only those facts that I believe are necessary to establish probable cause and does not include all the facts uncovered during the investigation.

RELEVANT STATUTES

5. This investigation concerns alleged violations of: 18 U.S.C. § 2251 (Sexual Exploitation of Children); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (knowing possession, access, conspiracy to access, or attempted possession or access with intent to view child pornography).

a. 18 U.S.C. § 2251 prohibits a person from employing, using, persuading, inducing, enticing or coercing a minor to engage in any sexually explicit conduct for the purpose of producing a visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

b. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

c. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

6. The following definitions apply to this Affidavit:
 - a. “Child erotica,” as used herein, means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.
 - b. “Child Pornography,” as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

- c. “Minor” means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).
- d. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
- e. “Computer Server” or “Server,” as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A DNS (domain name system) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.
- f. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage

devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks). Examples of computer hardware include, but are not limited to, central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants (“PDAs”), smart phones, iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), and portable media players.

- g. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- h. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- i. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
- j. “Mobile computing devices,” are handheld electronic devices used for storing data (such as names, addresses, music, photographs, appointments or notes) and utilizing computer programs. Some mobile computers also function as wireless communication devices and are used to access the Internet and send and receive e-mail. Mobile computers often include a memory card or other removable storage media for storing data and a keyboard and/or touch screen

for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Many users of these devices also use cloud storage applications to store data such as images and videos in order to back up data, duplicate data in order to access data from other devices, or to free up space on their device. Most mobile computers run computer software, giving them many of the same capabilities as personal computers. For example, mobile computers users can work with word-processing documents, spreadsheets, presentations, Internet browsing and chat applications. Mobile computers may also include global positioning system (“GPS”) technology for determining the location of the device. Mobile computing devices include, but are not limited to, laptops, tablets and smartphones. This type of Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and a mobile computer. As the amount of data that people store on their mobile devices has increased, smartphones and other mobile computing devices are also commonly synched with, or connected to, a desktop or laptop computer for backup data storage. This allows users to access selected data, such as photos, emails, contacts and documents, across multiple devices, or to recover this data if their mobile device is broken or lost.

- k. A “wireless telephone” (or mobile telephone, cellular telephone, or smartphone) is a handheld wireless device used for voice and data

communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

1. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- m. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers

including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

- n. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.
- o. “TOR” or “TOR Network”, also known as the “Onion Router”, is a network

of computers designed to facilitate anonymity. Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org. The Tor software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. It prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and it lets the user access sites which could otherwise be blocked. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP back through that Tor exit node IP. In that way, using the Tor

network operates similarly to a proxy server – that is, a computer through which communications are routed to obscure a user’s true location.

- p. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as thumb drives, flash drives, hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- q. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).
- r. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Computers and digital technology have revolutionized the way in which individuals interested in child pornography interact with one another. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

8. The development of computers and digital cameras has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

9. Individuals who access with intent to view and/or possess, receive, distribute or advertise child pornography can now transfer printed photographs into a computer-readable format with a scanner. Furthermore, with digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store over 100 gigabytes of data, which provide enough space to store thousands of high-resolution photographs. Video camcorders that once recorded video

onto tapes or mini-CDs can now save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Similarly, some current mobile computing devices, including wireless phones, can store up to a terabyte of data. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte (1000 gigabytes) external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them.)

11. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in

most cases.

12. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

BACKGROUND CONCERNING DARK NET AND CRYPTOCURRENCY

INVESTIGATIONS

13. The "clear" or "surface" web is part of the internet accessible to anyone with a standard browser and that standard web search engines can index. The deep web is the part of the internet whose contents are not indexed by standard web search engines. The dark net is a part of the deep web that not only cannot be discovered through a traditional search engine, but also has been intentionally hidden and is inaccessible through standard browsers and methods.

14. Dark net marketplaces operate on the dark net. These sites are generally only accessible through the input of specific addresses in a TOR browser. The dark net marketplaces function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods as well as the occasional sale of legal

products. Dark net vendors (also known as distributors) operate on these dark net markets as sellers of these goods. They provide detailed information about their wares on these sites, including listings of their drugs for sale, contact information (such as TOR-based email or encrypted messaging applications), and the prices and quantities of drugs for sale. Items purchased through dark net vendors are generally paid for in cryptocurrency such as Bitcoin. Cryptocurrency or virtual currency permits the anonymous exchange of unlimited amounts of digital currency to anyone in the world without the use of traditional banks or banking systems. Customers purchase these goods using a computer or smartphone.

15. Bitcoin (BTC)¹ is a type of virtual currency, circulated over the internet. Bitcoin are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency. Other currency includes Bitcoin Cash (“BCH”), Litecoin (“LTC”), Ethereum (“ETH” or “ether”), and Ripple (XRP). For ease of reference, the analysis below relating to Bitcoin generally applies to other types of cryptocurrencies (often collectively referred to as “Altcoins”).

16. Bitcoin are sent to and received from BTC “addresses.” A Bitcoin address is somewhat analogous to a bank account number and is represented as a case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key. This key is the equivalent of a password, or PIN, and is necessary to access the Bitcoin address. Only the holder of an address’ private key can authorize any transfers

¹ Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the currency. That practice is adopted here.

of bitcoin from that address to other Bitcoin addresses. Users can operate multiple BTC addresses at any given time and may use a unique Bitcoin address for each and every transaction.

17. To acquire bitcoin, a typical user purchases them from a virtual² currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (*e.g.*, U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information about their customers and verify their clients' identities.

18. To transfer bitcoin to another Bitcoin address, the sender transmits a transaction announcement, which is electronically signed with the sender's private key, across the peer-to-peer BTC network. To complete a transaction, a sender needs only the Bitcoin address of the receiving party and the sender's own private key. This information on its own rarely reflect any identifying information about either sender or recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain, a decentralized public ledger that records every Bitcoin transaction. The blockchain logs every Bitcoin address that has ever received bitcoin and maintains records of every transaction for each Bitcoin address.

19. While a Bitcoin address owner's identity is generally anonymous within the

² Bitcoins can accurately be referred to as a virtual, digital, and/or cryptographic currency.

blockchain (unless the owner opts to make information about the owner's Bitcoin address publicly available), investigators can use the blockchain to identify the owner of a particular Bitcoin address. Because the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators can sometimes trace transactions to third party companies that collect identifying information about their customers and are responsive to legal process.

20. In addition to Bitcoin and other cryptocurrencies, there are also tokens. Like Bitcoin and Altcoins, tokens use blockchain technology. Tokens are digital assets that are powered through smart contracts. While tokens theoretically can be used to represent any assets that are fungible and tradeable, they are often used as a commodity similar in some ways to stocks or options. In these scenarios, tokens are created and distributed through an Initial Coin Offering (ICO). Through an ICO, a venture offers a stock of specialized crypto tokens for sale with the promise that those tokens will operate as the medium of exchange when accessing services on a digital platform developed by the venture. The sale of tokens provides capital to fund the initial development of the digital platform, although no commitment is made as to the price of future services (in tokens or otherwise). In this sense, tokens are a fungible and potentially highly volatile unit of value that can be easy to obtain. Your affiant is aware that dark net distributors are increasingly using tokens as a means of laundering their illicit gains.

21. Your affiant is aware that individuals conducting business in this manner must use a computer or other electronic device, such as a smartphone, tablet, or computer to conduct transactions involving cryptocurrencies or tokens. Users of cryptocurrencies or tokens must establish electronic wallets to receive and send the bitcoin during these transactions. These wallets are electronic in nature and may be stored on mobile devices (phones or tablets), external

or removable media, or computers. They may also be stored on third party wallet providers (such as Armory). Individuals often associate email accounts with these wallet providers and store information relating to that wallet on their email account. Your affiant is also aware that individuals conducting business by bitcoin can back-up wallets to paper printouts that would contain information to restore the wallet in an electronic form (cold storage). Passwords for access to electronic wallets are typically complex and are often written down or saved in an accessible manner on paper or on some electronic device. They are also often stored on email accounts, cloud or shared drives stored online (such as Google Drive), and other online storage mediums.

PROBABLE CAUSE

22. On October 20, 2020, writer received records from Coinbase in response to a subpoena served on October 9, 2020. The subpoena requested records associated to bitcoin addresses known to be associated to dark net sites that advertise Child Sexual Abuse Material (CSAM) material. Upon reviewing the subpoena results, an account registered to JOSHUA GLOWACKI, was identified as sending bitcoin payments to an address associated with a dark net website that advertises CSAM material.

23. GLOWACKI is a registered sex offender in the state of Ohio. On May 21, 2019, GLOWACKI pled guilty, in Cuyahoga County, to charges of Pandering Sexually Oriented Matter Involving a Minor.

24. GLOWACKI, registered his account in Coinbase (GLOWACKI'S ACCOUNT) on November 16, 2019. GLOWACKI registered the account with email address jglowacki27@gmail.com (**Glowacki's Email**) and telephone number [REDACTED] As

displayed below, GLOWACKI provided his Ohio drivers license to Coinbase for verification purposes:



25. Records received pursuant to legal process served on AT&T revealed that telephone number [REDACTED] is registered to Matthew J Glowacki Jr, of [REDACTED] Cleveland, Ohio.

26. On December 24, 2019, GLOWACKI'S ACCOUNT sent two payments to bitcoin address 15WK91Jq47uFASfBGwvY6SSv6Vc7tEgZfJ (**BTC Address**). This address is associated to the dark net site hosted in the URL **childsivo3n3xzei.onion** (**Target URL**) which advertises itself as "terabytes of child porn private site".

27. Using blockchain analysis investigators were able to identify that **BTC Address** have received approximately 1.75 BTC (approximately \$12,000). Over 96% of the funds received in the wallet associated to BTC Address were sent to the virtual currency exchanger YoBit.net³.

3 YoBit.net is a virtual currency exchanger based in Rusia and does not repond to legal process.

28. Open searches for information associated to **BTC Address** revealed that this bitcoin address has been previously reported in the public website www.bitcoinabuse.com as follow: "TOR site advertising for child exploitation videos. Below is the ad US \$ 15 - After payment to the bitcoin address number: 15WK91Jq47uFASfBGwvY6SSv6Vc7tEgZfJ write the transaction number write to e-mail: video-child@secmail.pro we will send you access."

29. On February 20, 2020, Internet Watch Foundation Bitcoin (IWF)⁴, www.iwf.org.uk, reported that **BTC Address** has been identified as an address involved in child abuse material.

30. On October 27, 2020, investigators visited **Target URL** and identified the following:

- a. Upon accessing the website over a dozen images were loaded in the website.
- b. A review of the images displayed revealed possible child pornography.
- c. The files categorized as possible child pornography were evaluated to contain visual depictions of real minors engaged in sexually explicit conduct, including lascivious exhibition of the genitals or pubic area.
- d. The images and videos all depicted prepubescent female and male children exposing their genitalia or engaged in a sexual act with an adult male. Some of the images are further described below to provide an overview of what was found in the review:

⁴ The Internet Watch Foundation (IWF) is a registered charity based in Cambridgeshire, England. It states that its remit is "to minimise the availability of online sexual abuse content, specifically child sexual abuse images and videos hosted anywhere in the world and non-photographic child sexual abuse images hosted in the UK." Content inciting racial hatred was removed from the IWF's remit after a police website was set up for the purpose in April 2011.

- Image of a prepubescent female, approximately 11 to 14 years old, lying on her side, naked and with her legs apart.
 - Image of a prepubescent female, approximately 8 to 10 years old, on her hands and knees, and an adult male inserting his erect penis into the prepubescent female vagina from the rear.
 - Image of a naked prepubescent male, approximately 8 to 10 years old straddling a prepubescent female, approximately 8 to 10 years old who is lying on her back, appearing to have vaginal intercourse. A naked male is in the picture appearing to be observing and assisting the prepubescent male.
 - Image of a prepubescent female, approximately 8 to 10 years old, performing oral sex on an adult male.
- e. The website advertised “Access to 10 + terabytes of child porn private site.”
- f. At the time of the review, **Target URL** listed BTC address 1Gs7Aztizk2rNNSE6AbpK4K7yAFTCZKV9a (**BTC Address 2**) for payments. Users of the website are expected to send payment in form of BTC to the provided address prior to getting access to a larger collection. The website asked for users to send the transaction id associated to the payment to email address child-video@secmail.pro and “we will send you access.”
- g. Blockchain analysis conducted by investigators on **BTC Address 2** revealed that this address has been associated with the virtual currency exchanger YoBit.net.

- h. **BTC Address 2** has been identified by the IWF as an address involved in child abuse material.
- i. **Target URL** lists email addresses video-child@secmail.pro and child-video@secmail.pro for contact.

31. The images all depicted prepubescent female and male children exposing their genitalia or engaged in a sexual act with an adult male.

32. On August 13, 2020, investigators conducted surveillance at the TARGET PREMISES and confirmed the home was a single-family residence with white siding.

33. On February 18, 2021, investigators conducted surveillance at TARGET PREMISES and observed GLOWACKI utilizing a snowblower and a snow shovel in the driveway of TARGET PREMISES.

34. Records received pursuant to a court order requesting records associated to **Glowacki's Email** showed the following:

- a. **Glowacki's Email** was created on August 19, 2013 and is registered to Joshua Glowacki.
- b. Between November 9, 2020, and January 2, 2021, **Glowacki's Email** was accessed from IP address 108.94.129.177 multiple times.

35. Records received pursuant to legal process requesting records associated to IP address 108.94.129.177 revealed the following:

- a. IP addressed was assigned to TARGET PREMISES on November 5, 2020, at approximately 19:59 and was still assigned to TARGET PREMISES until at least February 24, 2020.

BIOMETRIC ACCESS TO DEVICE(S)

36. This warrant permits law enforcement agents to obtain from the person of JOSHUA GLOWACKI the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any devices requiring such biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to

five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

- c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face
- d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record

data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some

circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

- h. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the SUBJECT RESIDENCE; (2) hold the Device(s) found at the SUBJECT RESIDENCE in front of the face of the aforementioned person(s) to activate the facial

recognition feature; and/or (3) hold the Device(s) found at the SUBJECT RESIDENCE in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant. The proposed warrant does not authorize (nor does it prohibit) law enforcement to request that the aforementioned person state or otherwise provide the password or any other means that may be used to unlock or access the Device(s). Moreover, the proposed warrant does not authorize (nor does it prohibit) law enforcement to ask the aforementioned person(s) to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). That is, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires such person to provide such information; that is, the agents will make clear that any such request is voluntary/the person is free to refuse the request.

CONCLUSION

23. Based on the foregoing, there is probable cause to believe that 18 U.S.C. § 2251 (Sexual Exploitation of Children); 18 U.S.C. 2252A(a)(2)(A) and (b)(1) (receiving and distributing or conspiracy to receive and distribute or attempting to receive and distribute child


pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (knowing possession, access, attempted or conspiracy to access with intent to view child pornography); and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request this Court issue a search warrant for the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

24. Based on the information described above, there is probable cause to believe the information described in Attachment B constitutes evidence and instrumentalities of the above-mentioned crimes.



Special Agent Monica Hantz
Federal Bureau of Investigation

Sworn to via telephone after submission by reliable electronic means, pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3), this 19th day of March, 2021:



William H. Baughman, Jr.
United States Magistrate Judge